Coding Theory: Problem sheet 4

Solutions must be submitted by 12pm on Thursday 29 November 2007

1. Write down parity check matrices for the Hamming code Ham$(2, 4)$ and the extended Hamming code Ham$(2, 4)^+$ over Z_2. [4]

2. Let C be the Hamming code over Z_5 with parity-check matrix

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 \end{pmatrix}.$$

Decode the following words with respect to C: (i) 231022, (ii) 040404, (iii) 134233. [6]

3. Find the minimum distance of the linear code C over Z_2 with generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

[Hint: find a parity check matrix for the code.]

Prove that $C \neq C^\perp$ but that C is equivalent to $C^\perp$. [10]

4. Recall that a linear code C is *self-dual* if $C = C^\perp$. Prove that the extended Hamming code Ham$(2, 3)^+$ is self-dual. [6]

5. Let

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 2 & 1 & 1 & 2 \\ 1 & 2 & 0 & 2 & 1 & 1 \\ 1 & 1 & 2 & 0 & 2 & 1 \\ 1 & 1 & 1 & 2 & 0 & 2 \\ 1 & 2 & 1 & 1 & 2 & 0 \end{pmatrix}.$$

be a matrix with entries in Z_3. Check that $A = A^t$ and that $A^2 = -I_6$. Prove that

$$B = (I_6 \mid A) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & 1 & 1 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 2 & 0 & 2 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 2 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 1 & 1 & 2 & 0 \end{pmatrix}$$

is the generator matrix of a self-dual code C over Z_3. Also prove that the weight of each word of C is a multiple of 3. [12]

6. Determine whether the Hamming code $\mathrm{Ham}(3, 2)$ over Z_3 is equivalent to a cyclic code. [Hint: what are the cyclic codes of that length?] [8]

7. Let C be the cyclic code of length 15 over Z_2 with generator polynomial x^4+x^3+1. Prove that C is equivalent to the Hamming code $\mathrm{Ham}(2, 4)$. [Hint: find a parity-check matrix of C.] [8]

8. Factorize $x^8 - 1$ into irreducible factors over Z_3. Hence describe all cyclic codes of length 8 and dimension 4 over Z_3, in each case listing the generator polynomial. [10]

9. Factorize $x^6 - 1$ into irreducible factors over Z_5. Hence describe all cyclic codes of length 6 over Z_5, in each case listing the dimension and generator polynomial. [10]

10. The `MAPLE` syntax for factorizing a polynomial f into irreducible factors modulo a prime p is

```
> Factor(f) mod p;
```

(note the capital F). Using `MAPLE` describe all cyclic codes of length n over Z_p of length n (in each case listing the dimension and generator polynomial) for the following values of n and p: (i) $(n, p) = (11, 2)$, (ii) $(n, p) = (17, 2)$, (iii) $(n, p) = (23, 2)$, (iv) $(n, p) = (11, 3)$, (v) $(n, p) = (16, 3)$. (For (v) just determine the number of cyclic codes of each possible dimension; omit their generator polynomials — there are a lot of them!) [14]

11. Let $f(x) = 1 + x + x^2 + \cdots + x^{n-1}$ and let $g(x) \in Z_p[x]$. Prove that $g(x)f(x) = g(1)f(x)$ when both sides are regarded as elements of the truncated polynomial ring $Z_p[x]_n$. Hence prove that if C is a cyclic code then either C or $C^{\perp}$ contains the all-one word. [12]

12. (Challenge problem) Consider the code in question 5. Prove that C has minimum weight 6. Prove that the code C^{-} obtained from C by deleting the first entry of each word is a perfect 2-error correcting code of length 11 over Z_3.

RJC 6/11/2007